I claim:

1. A method for hiding auxiliary data in a media signal, the method comprising:

compressing a first media signal; and

embedding the first media signal into a second media signal.

2. The method of claim 1 wherein the first media signal is at least a part of the second media signal.

3. The method of claim 1 wherein the embedding includes associating a symbol with a sorting order, determining a sorting order of a block of samples, and modulating the sorting order of the block of samples as necessary to make the sorting order match the sorting order associated with a symbol to be embedded.

4. A computer readable medium on which is stored software for performing the method of claim 1.

5. A method of decoding auxiliary data that has been imperceptibly embedded into a host signal:

decoding the auxiliary signal, which represents a compressed version of the host signal;

decompressing the compressed version;

using the decompressed version to authenticate the host signal.

6. The method of claim 5 wherein the decoding includes using a sorting order decoder to analyze sorting order of selected blocks of samples, and to look up a symbol corresponding to the sorting order.

7. A computer readable medium on which is stored software for performing the method of claim 5.

8. The method of claim 5 wherein the decoding is performed on blocks of the host signal.

9. The method of claim 8 wherein auxiliary data decoded from one block of the host signal is used to authenticate another block of the host signal.

10. A method of watermarking media content comprising:
selecting non-overlapping blocks A, B and C of the media content;
losslessly compressing blocks B and C of the content to form compressed content;
watermark embedding the compressed content into block B of the media content to form a new block B';
creating a hash of block A and B';
watermark embedding the hash into block C to create a new block C'; and
combining blocks A, B' and C' to form watermarked media content.

11. The method of claim 10 wherein the media content is an image.

12. The method of claim 10 wherein the media content is an audio signal.

13. A computer readable medium having software for executing the method of claim 10.

14. A watermark decoder for decoding the hash from the watermarked media content created by the method of claim 10, the decoder operable to compare the hash with a new hash calculated from the watermarked media content to determine whether the watermarked media content is authentic.

15. The watermark decoder of claim 14 further including a decoder for reconstructing original un-watermarked media content by using watermark

decoding to extract the compressed content and decompressing the compressed content.

16. A computer readable medium on which is stored software for implementing the watermark decoder of claim 14.

17. A method for encoding a reversible watermark in a media signal comprising:

embedding a watermark message signal into a reference media signal to create a watermarked reference signal, where the watermark message signal includes information about a watermark embedder function used to embed the watermark message signal into the reference signal;

subtracting the reference signal from the watermarked reference signal to form a difference signal; and

adding the difference signal to a host media signal to embed the watermark message signal in the host signal;

wherein adding the difference signal is reversible by decoding the information about the watermark embedder function from the host media signal, using the information about the watermark embedder function to re-compute the difference signal, and subtracting the difference signal from the host media signal to restore the host signal.

18. The method of claim 17 further including:

computing a hash of the host signal; and including the hash in the watermark message signal such that the message signal includes the hash and the information about the watermark embedder function.

19. The method of claim 17 wherein the information about the watermark embedder function is a watermark durability parameter.

20. The method of claim 17 wherein the host signal is a still image.

21. The method of claim 20 wherein the reference signal is an image of substantially uniform pixel values.

22. The method of claim 21 wherein the reference signal comprises uniform pixel values at a mid-level between a range of possible pixel values between a lowest possible value and a highest possible value.

23. A computer readable medium on which is stored software for performing the method of claim 17.

24. A method for authenticating a watermarked media signal that has been watermarked using a watermark embedding function on an un-watermarked version of the media signal, comprising:

decoding a watermark message from the watermarked media signal, wherein the watermark message includes a hash of the un-watermarked media signal and watermark embedding information used by the watermark embedding function to create the watermarked media signal;

transforming the watermark embedding information and hash into a watermark difference signal using the watermark embedding function;

subtracting the watermark difference signal from the watermarked media signal to restore the un-watermarked media signal;

computing a new hash of the restored, un-watermarked media signal; and

comparing the new hash with the hash decoded from the watermarked media signal to determine the authenticity of the watermarked media signal.

25. The method of claim 24 wherein transforming includes watermark embedding a reference signal with the hash and watermark embedding information to compute a watermarked reference signal, computing a difference signal between the

watermarked reference signal and the reference signal to compute the watermark difference signal.

26. The method of claim 25 wherein the reference signal comprises an image having substantially uniform pixel values.

27. A computer readable medium on which is stored software for performing the method of claim 24.

28. A method for encoding a reversible watermark in a media signal comprising:

creating a watermark difference signal carrying information about a watermark embedder function used to embed the watermark message signal into the difference signal; and

adding the difference signal to a host media signal to embed the watermark message signal in the host signal;

wherein adding the difference signal is reversible by decoding the information about the watermark embedder function from the host media signal, using the information about the watermark embedder function to re-compute the difference signal, and subtracting the difference signal from the host media signal to restore the host signal.

29. A computer readable medium on which is stored software for performing the method of claim 28.

30. A method of hiding auxiliary data in a media signal, the method comprising:

dividing the media signal into blocks;

partitioning the media signal into two regions;

for a plurality of the blocks, compressing the media signal from a first region of a block and embedding redundant instances of the compressed media signal of the block into a second region of two or more blocks.

31. The method of claim 30 including:

for a plurality of blocks, computing a fragile hash of the first region of the media signal for the block and embedding the fragile hash into a second region of one or more blocks.

32. The method of claim 31 wherein the fragile hash comprises a fragile hash of the compressed media signal of the block.

33. The method of claim 31 wherein the second region of blocks in the media signal are partitioned into sub-regions and the sub-regions for the blocks are embedded with a fragile hash from another block and instances of the compressed media signal from the first region of other blocks.

34. A computer readable media on which is stored software for performing the method of claim 30.

35. The method of claim 30 wherein the second region comprises one or more least significant bits of data samples of the media signal, and embedding of redundant instances comprises replacing least significant bits of the data samples.

36. The method of claim 30 wherein the redundant instances are scrambled before the embedding using a key.

37. The method of claim 30 wherein the redundant instances are mapped to different blocks for embedding according to a permutation.

38. A method of authenticating a media signal using hidden embedded data in the media signal, the method comprising:

dividing the media signal into blocks;

partitioning the blocks into regions;

for a plurality of blocks, extracting hidden compressed bit streams of a first region other blocks from a second region in the blocks;

for a plurality of blocks, evaluating whether a block is altered by comparing the extracted compressed bit streams for a block with the media signal in the first region of the block; and

when an altered block is detected by the comparison, using a fragile hash to identify location of altered data, and using an extracted compressed bit stream to replace the altered data.